Introduction to Shibboleth

Steve Carmody

Brown University

Kentucky Education Network

July 6, 2007

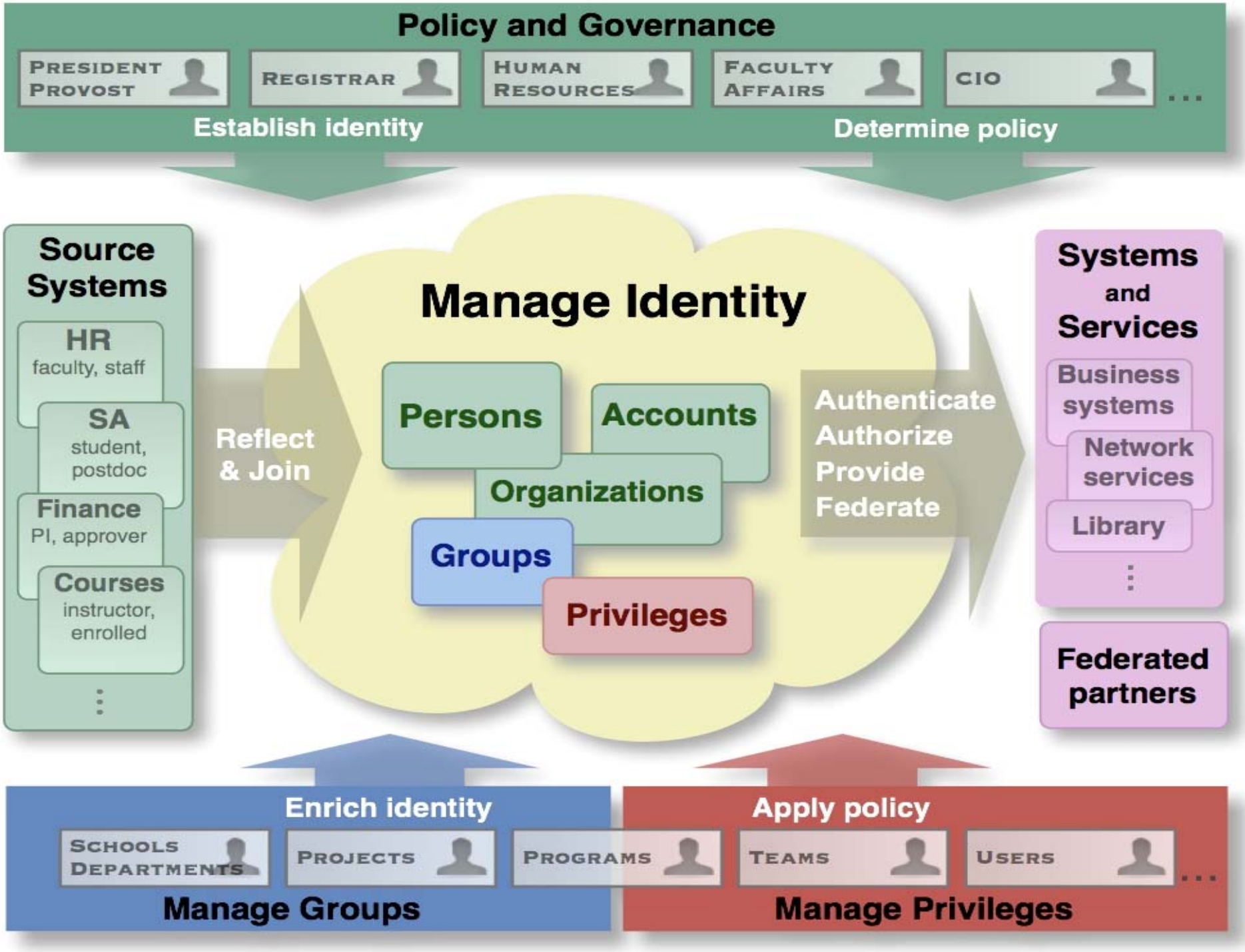
EDUCAUSE INTERNET2 nmi-edit

Topics

- The MACE Identity Management Model
- What is Shibboleth…
- The User Experience with Shibboleth
- Status….
- The Process of Deploying Shibboleth

What is Identity Management?

- *"A set of processes, and a supporting infrastructure, for the creation, maintenance, and use of digital identities." (Burton Group)*
- **It is more than account creation, more than directories, authentication, access controls, etc.**
- **It includes policy, process, governance, trust, and new ways of thinking about I.T.**


Policy and Governance
President
Provost
Registrar
Human Resources
Faculty Affairs
CIO
...
Establish identity
Determine policy
Source Systems
HR
faculty, staff
SA
student, postdoc
Finance
PI, approver
Courses
instructor, enrolled
Reflect & Join
Manage Identity
Persons
Accounts
Organizations
Groups
Privileges
Authenticate
Authorize
Provide
Federate
Systems and Services
Business systems
Network services
Library
Federated partners
Enrich identity
Schools
Departments
Projects
Programs
Manage Groups
Apply policy
Teams
Users
Manage Privileges

First, a few terms…

- **Authentication – "The process by which you prove your identity to another party…" (Cornell University)**
- **Authorization – "The process of determining a user's right to access a resource." (the MAMS project - Australia)**
- **Credential – "An object that is verified when presented to the verifier in an authentication transaction." (Webopedia, OMB)**
- **Federation – "A collection of organizations that agree to interoperate under a certain ruleset." (SWITCH)**

A few *more* terms…

- **Identification/Vetting – "The process by which information about a person is gathered and used to provide some level of assurance that the person is who they claim to be." (NMI-EDIT)**
- **Level of Assurance (LoA) – "Describes the degree of certainty that the user has presented an identifier (a credential in this context) that refers to his or her identity." (NMI-EDIT)**
- **Reflect & Join – "Accumulating, maintaining, and refreshing data of interest from authoritative source systems and consolidating it into a cohesive whole that represents an established identity."**

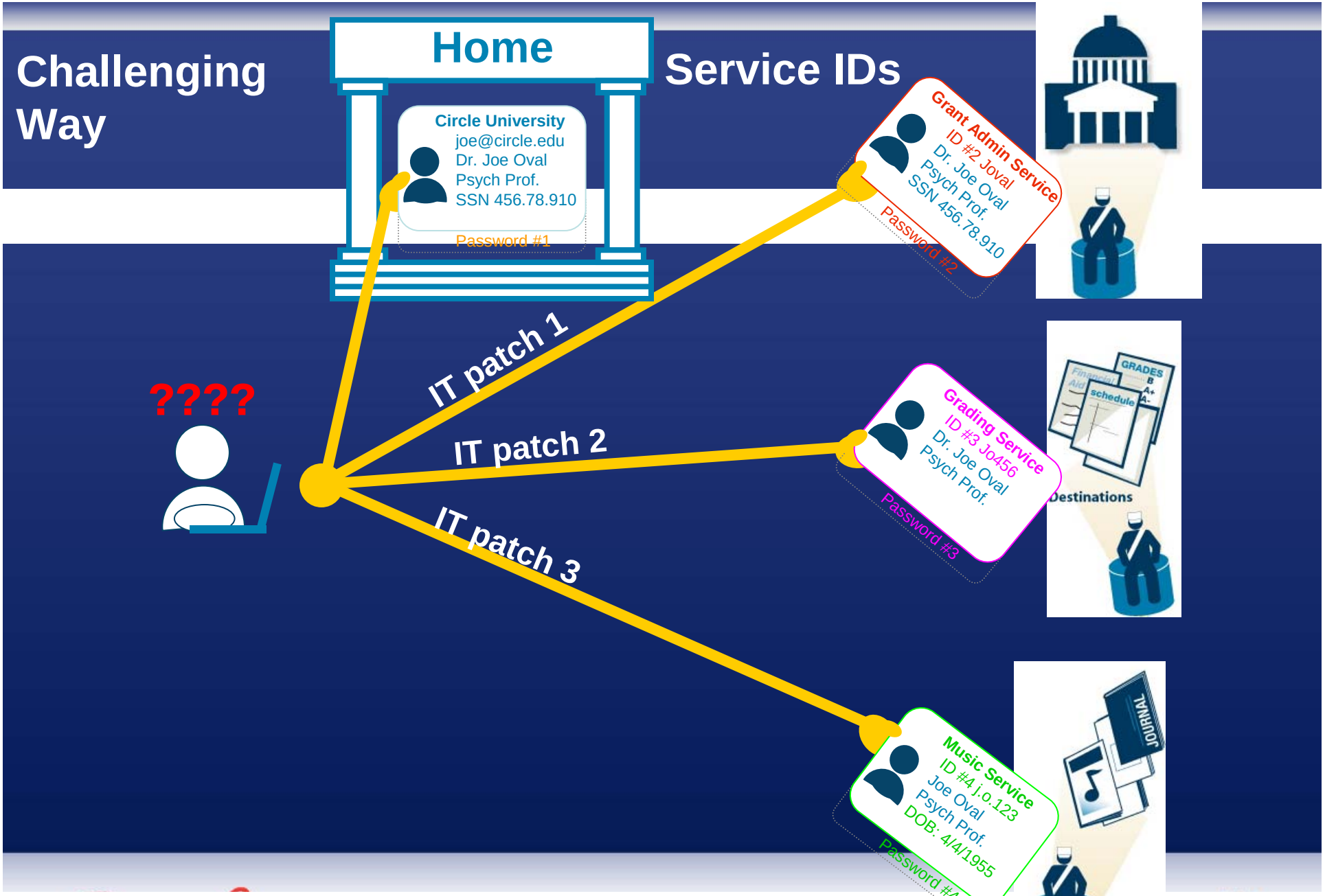
What is Shibboleth?

- An open source standards-based Web Single Sign-On (SSO) package
- Leverages local Identity Management system to enable access to campus and external applications
- Protects your data and your users' privacy
- Helps your service partners
- Plays well with others

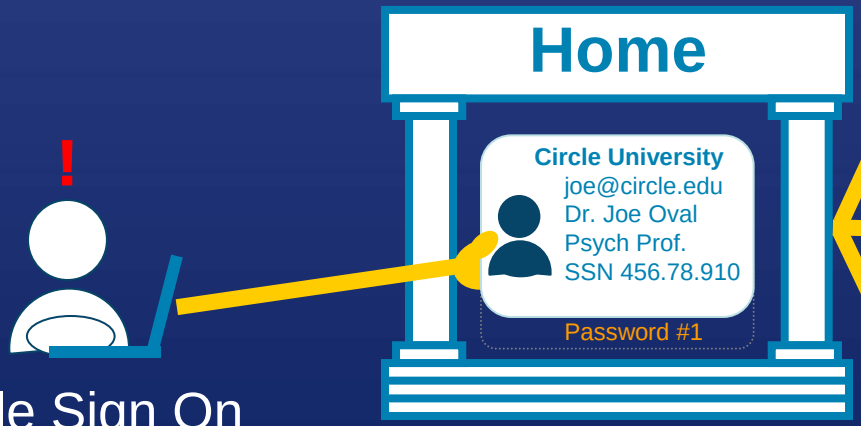
Key Concepts - Shibboleth in Your Environment

- Web Single SignOn
- Standards Based (SAML and ADFS)
- SSO w/Attribute-Based Single Sign-On
- Tools to Manage Privacy
- Federated Administration

Challenging Way



Federated Way



1. Single Sign On
2. Services no longer manage user accounts & personal data stores
3. Reduced Help Desk load
4. Standards-based Technology
5. Home Org controls privacy

Key Concepts - Shibboleth in Your Environment

- **Framework for a Variety of Policy and Management Models**
  - Intra-campus
  - Federations
  - Bilateral
- **Extensible Authentication and Attribute Sharing**
  - Federation defines syntax and semantics of common Attribute/Value pairs
  - Two parties can define custom attributes

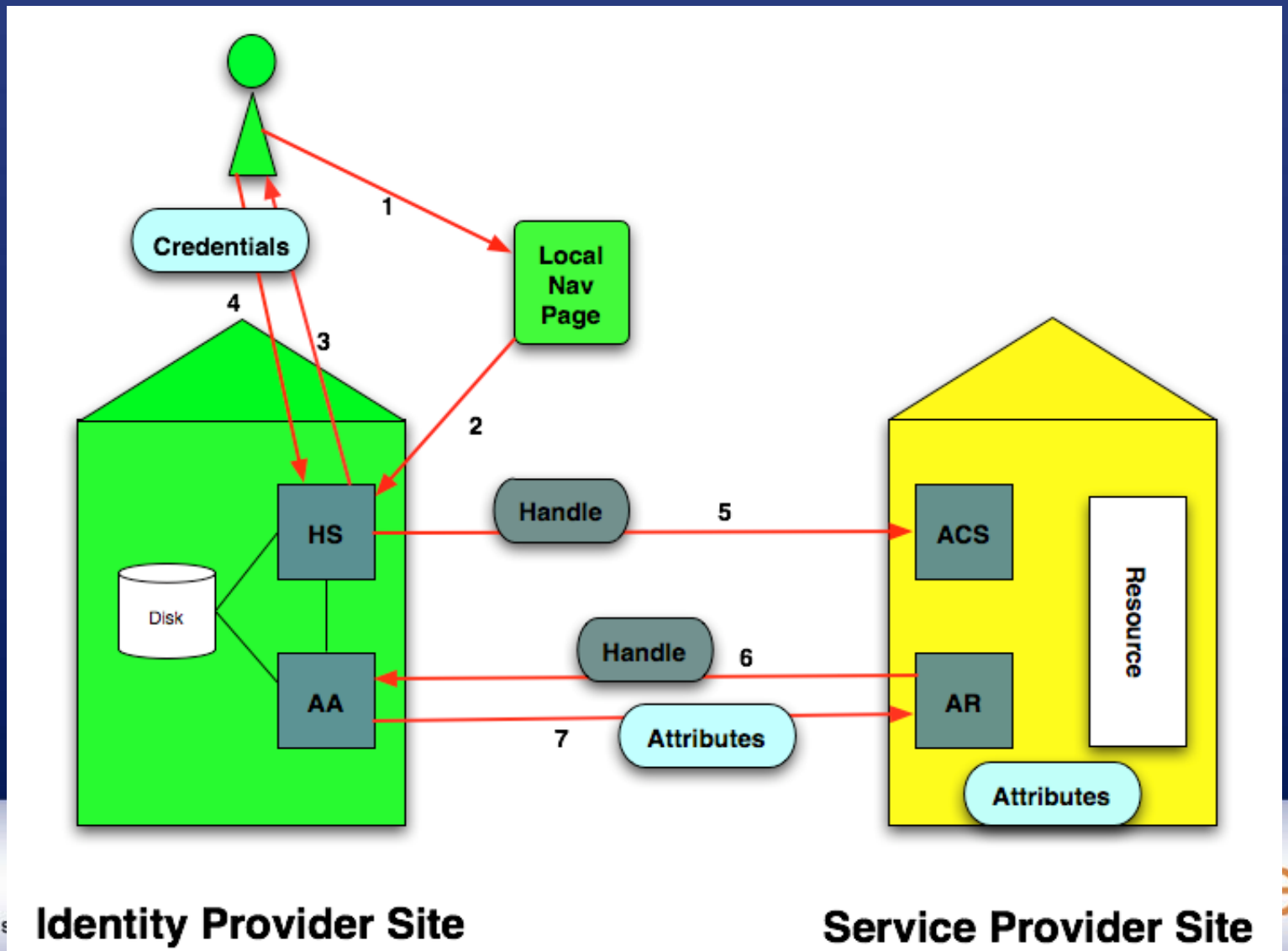
Shibboleth Value-Add compared to Other SAML Implementations

- Support for multiple protocols
- Management of Attribute Release (site, group, user Attribute Release Policies (ARPs))
- Management of Attribute Acceptance
- *Real* support for the concept of Federations
- Better support for application integration (eg lazy sessions)

Shibboleth -- How Does it Work?

- **Intra-campus Web SSO**
- **Access to external services**

Basic Browser Flow
Intra-Campus Web SSO

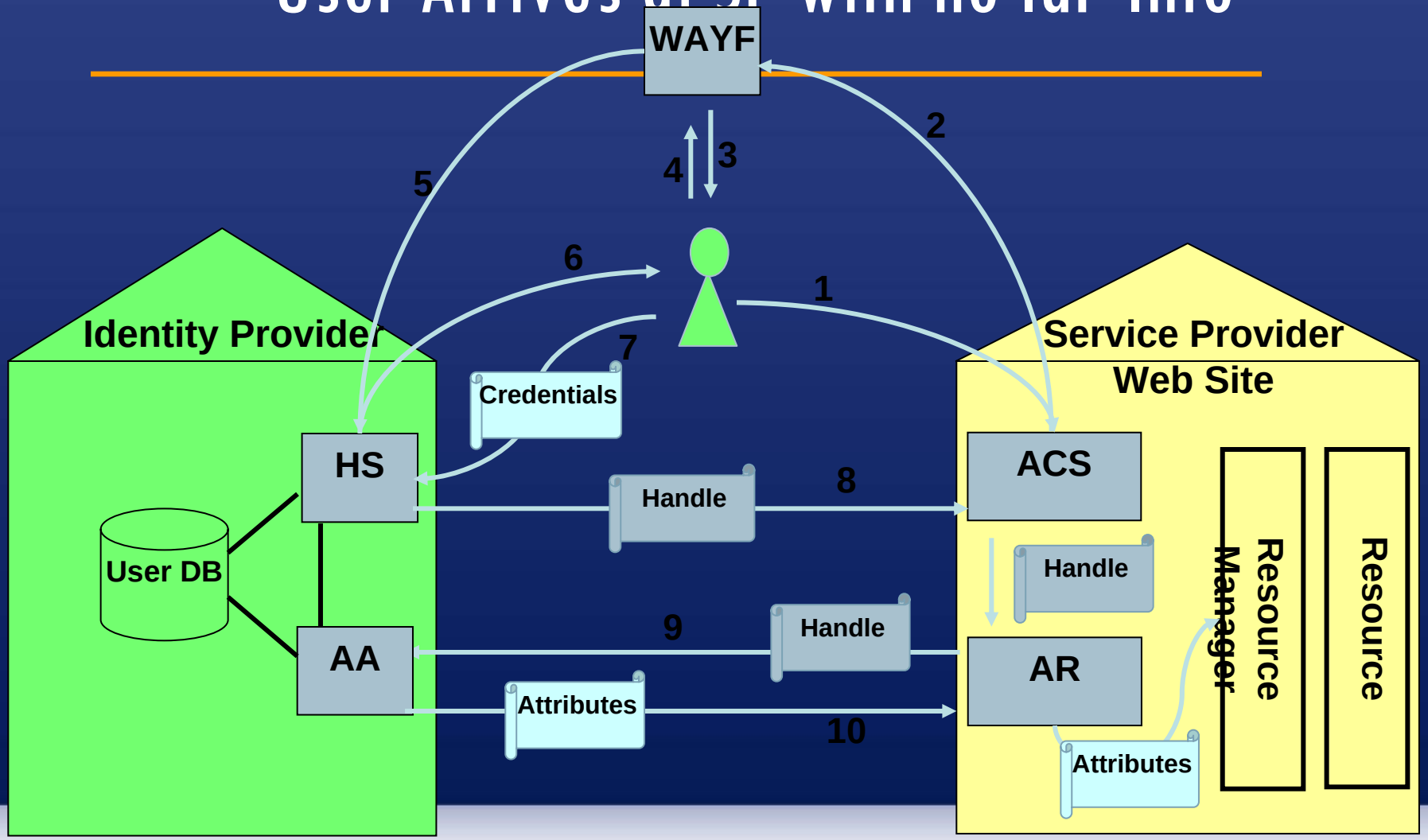


Shibboleth -- How Does it Work?
Accessing External Services

- 1. User arrives at Service Provider with NO indication of home site
- 2. SP redirects to WAYF; parameters include ACS url
- 3. WAYF presents list of Identity Providers in the Federation
- 4. User selects home site; is redirected to IdP; url parameters are passed through transparently
- 5. User arrives at IdP… continue as before

Advanced Flow

User Arrives at SP with no IdP Info



Demo!

Deploying Shibboleth in Four Stages

- Intra-campus Web SSO
- Intra-campus delivery of Attributes
- Federated Operation
- Inter-Federation Operation

- Operating a "Virtual" IdP

Shibboleth Status….

- **Worldwide Deploys**
- **US Deploys**
- **Shibboleth-enabled Vendors**

Worldwide Adoption in the Higher Ed Space

- Finland
- Sweden
- Denmark
- Germany
- Switzerland
- Greece
- The Netherlands
- Belgium
- France
- Spain
- The UK
- Australia
- New Zealand
- Canada
- The US

Adoption in US Higher Ed

- **InCommon**
- **Growing number of "state-wide" Federations**
- **Other Interesting Stories**
  - Texas Digital Library (TDL)
  - Database of Recorded American Music (http://dram.nyu.edu/)
  - University of Maryland System (16 campuses)
- **Library/IT Group**
  - Five campuses
  - Exploring approaches to deploy issues perceived by librarians
  - Have worked through most of the identified issues

Adoption in K12, Libraries

- **The UK - BECTA Project**
  - http://becta.org.uk/
  - Shibboleth adopted as a standard countrywide
  - -- following pilot in London with 50,000 students
  - Developing use cases for integration of SIF and Shibboleth
- **OhioLink**

Services Supporting Shibboleth

- **Google Apps for Education**
- **Course Management Systems**
  - BlackBoard
  - WebCT
  - Sakai
- **TurnItIn**
- **Information Providers**
  - Elsevier, EBSCO, JSTOR, OVID, CSA, Exlibris, Thomson Learning, etc

Questions?

www.internet2.edu